ferma

FEDERATION OF
EUROPEAN RISK
MANAGEMENT
ASSOCIATIONS

CADRE DE RÉFÉRENCE DE LA GESTION DES RISQUES

Introduction

Le Cadre de Référence de la Gestion des Risques est l'œuvre d'un groupe de travail composé des principaux organismes de la gestion des risques au Royaume Uni : l' Institute of Risk Management (IRM), l'Association of Insurance and Risk Managers (AIRMIC) et le National Forum for Risk Management in the Public Sector (ALARM).

Le groupe de travail a par ailleurs consulté et associé à ses travaux de nombreux professionnels ou enseignants concernés par la gestion des risques.

La gestion des risques est une discipline en développement rapide. De nombreuses définitions et différents points de vues existent sur ce qu'elle représente ou implique ainsi que sur la manière de la conduire. Une forme de cadre de référence est donc nécessaire pour préciser :

- *la terminologie,*
- *le processus de déploiement de la gestion des risques,*
- *l'organisation de la gestion des risques,*
- *l'objectif de la gestion des risques.*

Il est important de souligner que ce cadre de référence prend en compte le fait que certains risques comportent à la fois une part positive et une part négative.
La gestion des risques concerne les entreprises privées et les organismes publics, mais aussi toutes les organisations dont l'activité entraîne des conséquences à court ou long terme.

Menaces et opportunités s'évalueront non seulement du point de vue de l'activité elle-même mais aussi du point de vue de l'ensemble des parties prenantes qui pourraient être affectées.
Il existe de nombreuses manières pour atteindre les objectifs de la gestion des risques et il serait impossible de les énumérer toutes ici.
C'est pourquoi ce cadre de référence n'a pas vocation à être prescripteur ni à poser les bases d'un processus de certification. En revanche, les organisations pourront s'appuyer sur les différentes composantes de ce cadre de référence pour rendre compte de leur conformité. Ce cadre de Référence représente les meilleures pratiques actuelles à l'aune desquelles les organisations peuvent se mesurer.
Autant que possible, le cadre de référence utilise la terminologie présentée par l'International Organisation for Standardisation (ISO) dans son récent document ISO/IEC Guide 73 Risk Management – Vocabulary – Guidelines for use in standards.
Compte tenu des évolutions rapides dans ce domaine, les auteurs du présent document apprécieraient les observations ou commentaires des organisations qui l'utiliseront. Il est prévu de le faire évoluer à la lumière des meilleures pratiques.

1. Risque

La norme ISO/IEC Guide 73 définit le risque comme la combinaison de la probabilité d'un événement et des conséquences de celui-ci.
Le simple fait d'entreprendre ouvre la possibilité d'évènements dont les conséquences sont potentiellement bénéfiques (aléa positif) ou préjudiciables (aléa négatif).
On s'accorde de plus en plus à reconnaître que la gestion du risque s'intéresse à celui-ci sous les deux aspects de l'aléa positif et de l'aléa négatif. C'est pourquoi le présent document adopte les deux perspectives.
Dans le domaine de l'hygiène et la sécurité ou de la sûreté, les conséquences sont en général uniquement négatives et donc la gestion de ce type de risque est centrée sur leur prévention et leur atténuation.

2. Gestion du risque

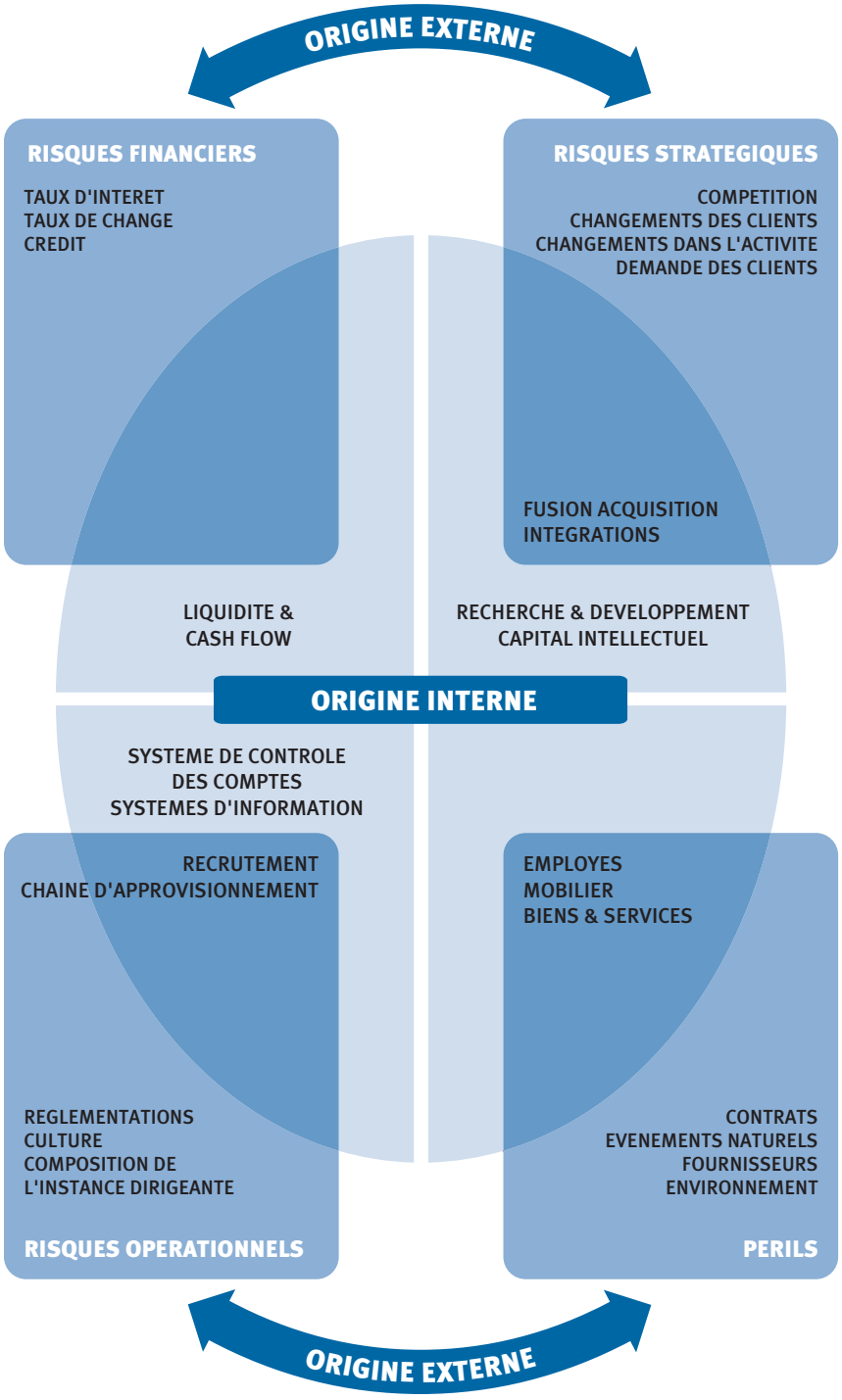
La gestion du risque fait partie intégrante de la mise en oeuvre de la stratégie de toute organisation. C'est le processus par lequel les organisations traitent méthodiquement les risques qui s'attachent à leurs activités et recherche ainsi des bénéfices durables dans le cadre de ces activités, considérées individuellement ou bien dans leur ensemble.
La gestion du risque est centrée sur l'identification et le traitement des risques. Elle a pour objectif d'ajouter le maximum de valeur durable à chaque activité de l'organisation. Elle mobilise la compréhension des aléas positifs ou négatifs qui dérivent de tous les facteurs qui peuvent affecter l'organisation. Elle augmente la probabilité de succès et réduit la probabilité d'échec et l'incertitude qui s'y attache.
La gestion du risque devrait être un processus continu d'amélioration qui commence avec la définition de la stratégie et se poursuit avec l'exécution de celle-ci. Elle devrait traiter systématiquement de tous les risques qui entourent les activités de l'organisation, que celles-ci soient passées, présentes ou surtout futures.
La gestion du risque doit faire partie intégrante de la culture de l'organisation et disposer d'une politique efficace et d'un programme d'actions soutenu et suivi par la direction au plus haut niveau. Lors de son exécution la stratégie de gestion du risque doit se décliner en objectifs tactiques et opérationnels et à ce titre la description de poste de chaque employé(e) ou responsable doit rappeler le rôle de cette personne dans la gestion des risques. Ceci encourage la transparence des responsabilités, la mesure des performances et leur sanction. L'efficacité opérationnelle est alors promue à tous les niveaux.

2.1 Facteurs Externes et Internes

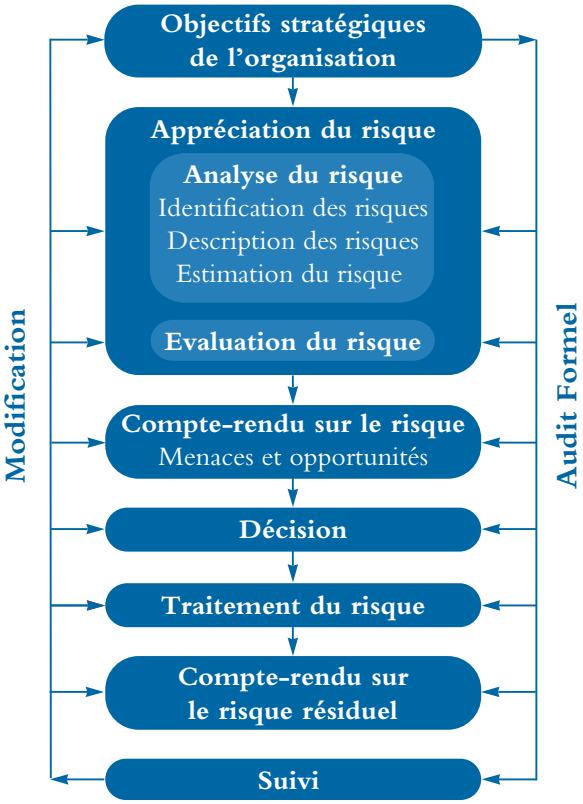
Les risques auxquels fait face une organisation sont d'origine interne ou externe.

Le diagramme au verso propose des exemples des principaux risques, et montre que certains d'entre eux répondent à des facteurs à la fois internes et externe : de ce fait ces zones se recoupent. Le classement des risques peut être affiné en distinguant par exemple les risque purs et ceux d'ordre stratégique, financier, opérationnel et cetera.

2.1 Exemples de facteurs Externes et Internes



2.2 Le Processus de gestion des Risques



La gestion du risque protège le patrimoine de l'organisation et crée de la valeur pour celle-ci et ses parties prenantes en :

- *fournissant un cadre méthodologique qui permet à toute activité future d'être mise en place de façon cohérente et maîtrisée,*
- *améliorant le processus des décisions, leur planification et leur hiérarchisation par une compréhension exhaustive et structurée des activités de l'organisation, de la volatilité de ses résultats et par l'analyse des opportunités ou menaces sur ses projets,*
- *contribuant à l'optimisation de l'utilisation/allocation du capital et des ressources dans l'organisation,*
- *réduisant la volatilité dans les secteurs non essentiels de l'organisation,*
- *protégeant et augmentant le patrimoine et l'image de marque de l'organisation,*
- *développant et soutenant le potentiel des employés et le capital de connaissance de l'organisation,*
- *optimisant l'efficience opérationnelle.*

3. Appréciation du risque

L'appréciation du risque est définie par le Guide ISO/IEC 73 comme le processus général d'analyse du risque et d'évaluation du risque. ***(cf. appendice)***

4. Analyse du risque

4.1 Identification des risques

L'identification des risques vise à identifier l'exposition d'une organisation à l'incertitude. Elle requiert une connaissance précise de l'organisation, des marchés où celle-ci opère, de son environnement juridique, social, politique et culturel. Elle requiert également de développer une solide compréhension de ses objectifs stratégiques et opérationnels, des facteurs critiques de succès et des menaces et opportunités qui s'y rapportent.
L'identification des risques requiert une approche méthodique pour garantir que chaque activité significative de l'organisation a été identifiée et que chaque risque qui en découle a bien reçu une définition. Toute volatilité associée à ces activités sera identifiée et classée dans une catégorie.

Les activités et les décisions de l'organisation peuvent être classées dans un éventail de catégories, dont par exemple :

- *stratégique : concerne les objectifs stratégiques à long terme de l'organisation; peut être affectée par des facteurs tels que disponibilité des capitaux, risques politiques ou souverains, changements légaux et réglementaires, réputation et changements dans l'environnement matériel,*
- *opérationnelle : concerne les questions quotidiennes auxquelles l'organisation est confrontée alors qu'elle poursuit ses objectifs stratégiques,*
- *financière : concerne la gestion et la maîtrise efficace des finances de l'organisation, et les effets de facteurs externes comme la disponibilité du crédit ou encore les fluctuations des taux de change, des taux d'intérêts ou encore d'autres références de marché,*
- *gestion des connaissances : concerne la gestion et de la maîtrise efficace des connaissances et des savoirs, de leur production, de leur protection, et de leur communication; cette catégorie peut être affectée par des facteurs externes comme l'usage non autorisé ou la violation de propriété intellectuelle, les pannes de secteur électriques ou encore l'apparition de technologies concurrentes; au nombre des facteurs internes figurent les défaut de fonctionnement informatique ou la perte de personnes clef,*
- *conformité : concerne entre autres l'hygiène, la sécurité et l'environnement, les lois sur la publicité et la protection des consommateurs, la protection des données, les pratiques en matière d'emploi et les questions réglementaires.*

Même si l'identification des risques peut être menée par des conseils externes, une approche interne sera probablement plus efficace si elle est dotée d'un ensemble d'outils et de méthodes cohérents, coordonnés et bien communiqués (cf. appendice, page 14). Il est essentiel que les acteurs internes soient les "propriétaires" du processus de gestion des risques.

4.2 Description des Risques

La description des risques consiste à présenter les risques identifiés, dans format structuré comme par exemple un tableau. Le tableau de description des risques 4.2.1 peut faciliter la description et l'évaluation de certains risques. La structure de ce format sera conçue avec soin pour s'assurer que les risques sont bien identifiés, décrits et appréciés exhaustivement et avec précision. En examinant les conséquences et la probabilité de chaque risque présenté dans le tableau, il devrait être possible de déterminer les risques clefs qui doivent être analysés plus en détail. L'identification des risques liés aux activités économiques et à la prise de décision peut recourir à des catégories comme "stratégique", "projet/tactique" ou encore "opérationnel". Il est important d'intégrer la gestion des risques dans chaque projet spécifique dès sa conception et pendant toute sa durée de vie.

4.2.1 Table - Description des Risques

1. Nom du Risque	
2. Portée du Risque	description qualitative des évènements, taille, type, nombre et interdépendances
3. Nature du Risque	En général stratégique, opérationnelle, financière, liée aux connaissances ou à la conformité
4. Parties prenantes	Parties prenantes et leurs attentes
5. Quantification du Risque	Importance et Probabilité
6. Tolérance/Appétence· pour le Risque	Perte potentielle et impact financier du risque Valeur à risque Probabilité et amplitude des gains/pertes potentielles Objectif(s) de la maîtrise des risques et niveau désiré de performance
7. Traitement du risque & Mécanismes de maîtrise	Principaux moyens par quoi le risque est actuellement géré Degré de confiance dans les moyens de maîtrise en place Identification des protocoles pour la surveillance des risques et leur examen
8. Actions d'amélioration possibles	Recommandations pour réduire le risque
9. Développement de la Stratégie et de Politique face au Risque	Identification de la fonction responsable de développer la stratégie et la politique face à ce risque

4.3 Estimation du risque

L'évaluation du risque peut être quantitative, semi-quantitative ou qualitative en termes de probabilité d'occurrence et de conséquences possibles.
Par exemple, les conséquences à la fois en terme de menaces (aléa négatif) et d'opportunités (aléa positif) peuvent être qualifiées de fortes, moyennes ou faibles (table 4.3.1). La probabilité peut se qualifier de haute, moyenne ou faible mais exige différentes définitions selon qu'il s'agit de menace ou d'opportunité (voir les tableaux 4.3.2 et 4.3.3).

Des exemples figurent dans les tableaux au verso. Les mesures les plus adaptées pour les conséquences et les probabilités peuvent varier d'une organisation a une autre.
Par exemple, beaucoup d'organisations jugent qu'évaluer les conséquences et les probabilités comme fortes, moyennes ou faibles selon une matrice 3x3 répond tout à fait leurs besoins. D'autres organisations préfèreront une matrice 5x5.

Table 4.3.1 Conséquences - Menaces et Opportunités

Fort	Impact financier sur l'organisation susceptible d'excéder €x. Impact significatif sur la stratégie ou les activités opérationnelles de l'organisation. Parties prenantes fortement préoccupées.
Moyen	Impact financier sur l'organisation compris entre €y et €x. Impact modéré sur la stratégie ou les activités opérationnelles de l'organisation. Parties Prenantes modérément préoccupées.
Faible	Impact financier sur l'organisation susceptible inférieur à €y Faible impact sur la stratégie ou les activités opérationnelles de l'organisation. Parties Prenantes faiblement préoccupées

Table 4.3.2 Probabilité d'Occurrence - Menaces

Estimation	Description	Indicateurs
Forte (Probable)	Susceptible de survenir chaque année ou plus de 25% de chances de survenir.	A le potentiel de survenir plusieurs fois dans la période considérée (par exemple dix ans). S'est produit récemment.
Modérée (Possible)	Susceptible de survenir dans les dix prochaines années ou moins de 25% de chances de survenir.	Pourrait survenir plus d'une fois dans la période considérée (par exemple dix ans). Peut être difficile à maîtriser en raison d'influences externes. Y -a-t-il un historique de survenance ?
Faible (peu probable)	Peu susceptible de survenir dans les dix prochaines années ou moins de 2% de chances de survenir.	Ne s'est pas encore produit. Peu susceptible de survenir.

Table 4.3.3 Probabilité d'Occurrence - Opportunités

Estimation	Description	Indicateurs
Forte (Probable)	Issue favorable probable dans l'année ou plus de 75% de chances de survenir.	Opportunité claire et raisonnablement certaine, devant se réaliser à court terme sur la base des processus de gestion actuels.
Modérée (Possible)	Perspective raisonnablement d'issue favorable dans l'année ou entre 25% et 75% de chances de survenir.	Opportunités qui ne sont pas hors d'atteinte mais demande une gestion attentive. Opportunités pouvant survenir en dépassement des résultats planifiés.
Faible (peu probable)	Quelques chances d'issue favorable dans l'année ou moins de 2% de chances de survenir.	Opportunité éventuelle qui demande encore à être investiguée complètement par la direction. Opportunité à faible probabilité de succès compte tenu des ressources qui lui sont allouées actuellement.

4.4 Méthodes et techniques d'analyse du risque

Un éventail de techniques peuvent servir à analyser les risques. Elles peuvent être spécifiques à l'aléa positif ou à l'aléa négatif ou bien au contraire convenir aux deux. ***(Voir Appendice)***.

4.5 Profil de risque

Le résultat de l'analyse du risque peut servir à produire un profil de risque qui donne une note d'importance à chaque risque et permet ainsi de déterminer les risques qui demandent un effort de traitement prioritaire. Un tel profil classe les risques identifiés et met ainsi en évidence leurs importances relatives.
Ce processus fournit la correspondance entre les risques et les secteurs d'activités, décrit les principaux moyens de maîtrise des risques en place et indique les secteurs où le niveau d'investissement dans la maîtrise du risque pourrait être augmenté, diminué ou re-proportionné.
Une bonne définition des responsabilités aide à faire reconnaître clairement le/la "propriétaire" de chaque risque et à assurer que les ressources de gestion appropriées sont correctement allouées.

5. Evaluation du risque

Après avoir analysé les risques, il est nécessaire de comparer les risques estimés aux critères de risque que l'organisation a établis. Les critères de risque peuvent comprendre les coûts et bénéfices associés, les contraintes juridiques, les facteurs socio-économiques et environnementaux, les préoccupations des parties prenantes, et cetera. Par conséquent l'évaluation du risque aide à décider de l'importance de chaque risque spécifique pour l'organisation, et à déterminer s'il convient d'accepter ce risque en l'état ou bien de le traiter.

6. Traitement du risque

Le processus de traitement du risque consiste à sélectionner et mettre en place des mesures propres à modifier le risque. Le traitement du risque a pour principales composantes la maîtrise et l'atténuation du risque, mais il ne s'y limite pas et s'étend entre autres à l'évitement, au transfert et à son financement du risque, et cetera.

NOTE: Dans ce cadre de référence, le financement du risque fait référence aux mécanismes (par exemple programmes d'assurance) de financement des conséquences financières du risque. En général le terme de financement du risque ne se rapporte pas au financement de la mise en place du traitement du risque (comme défini par le guide 73 d'ISO/IEC).

Tout système de traitement de risque doit assurer au minimum :

- *le bon fonctionnement de l'organisation,*
- *l'efficacité du système de contrôle interne,*
- *la conformité avec les lois et les règlements.*

Le processus d'analyse de risque aide au bon fonctionnement de l'organisation en identifiant les risques qui exigent l'attention des responsables. Ceux-ci devront déterminer les actions de maîtrise du risque qui sont prioritaires en terme de bénéfice potentiel pour l'organisation.

L'efficacité du système de contrôle interne se mesure au degré d'élimination ou de réduction du risque que procurent les mesures de maîtrise proposées.
L'efficacité économique du système de contrôle interne dépend du rapport entre les coûts d'implémentation de celui-ci et les bénéfices attendus de la réduction du risque.

Pour évaluer un projet de dispositif de maîtrise des risques, il convient de mesurer et de comparer :

- *l'effet économique potentiel si aucune mesure n'est prise,*
- *le coût de l'action (ou des actions) proposée(s).*

Invariablement ceci demande des informations et des hypothèses plus détaillées que celles dont on dispose dans l'immédiat.
Tout d'abord il convient d'établir le coût de mise en place, avec une certaine précision dans la mesure où ce chiffre devient rapidement la référence de base pour la mesure de la rentabilité du dispositif. Il convient également d'évaluer la perte escomptée si les mesures proposées ne sont pas prises. Après comparaison, les responsables peuvent décider ou non de mettre en place les mesures de maîtrise du risque étudiées.
La conformité avec les lois et les règlements ne peut pas se discuter. Une organisation doit comprendre les lois auxquelles elle est soumise et doit mettre en place un système de contrôle pour s'assurer de sa conformité. Une certaine flexibilité n'est possible que lorsque le coût de réduction d'un risque est en disproportion totale avec celui-ci.
Une méthode pour se protéger financièrement contre l'impact du risque réside dans le financement du risque, qui comprend l'assurance. Cependant, il faut noter que certaines pertes sont non-assurables comme par exemple certains coûts liés à la santé, aux conditions de travail, à la sûreté ou aux incidents environnementaux, qui peuvent comporter des atteintes au moral du personnel et à la réputation de l'organisation.

7. Compte-rendu et Communication relatifs au risque

7.1 Compte rendu Interne

Le processus de gestion des risques fournit des informations différentes aux différents niveaux de l'organisation.

L'instance dirigeante devrait :

- *connaître les risques les plus significatifs auxquels l'organisation fait face,*
- *connaître les effets potentiel de la non réalisation des fourchettes de performance prévues sur la valeur actionnariale,*
- *s'assurer que le niveau de sensibilisation aux risques est approprié dans toute l'organisation,*
- *savoir comment l'organisation gérerait une crise,*
- *connaître le degré de la confiance des parties prenantes de l'organisation,*
- *savoir comment gérer les communications avec la communauté des investisseurs s'il y a lieu,*
- *être assuré que le processus de gestion des risques fonctionne efficacement,*
- *produire une politique de gestion des risques écrite qui définisse l'approche générale et les responsabilités.*

Les Unités Opérationnelles devraient :

- *se tenir informées des risques qui relèvent de leur responsabilité, de leurs impacts possibles sur d'autres secteurs et inversement de l'effet des risques d'autres secteurs sur elles-mêmes,*
- *disposer d'indicateurs de performance qui leur permettent, de surveiller les activités clef, les données financières clef et les progrès vers les objectifs. Ces indicateurs doivent permettre d'identifier les développements qui nécessitent une intervention (par exemple : prévisions et budgets),*
- *disposer des systèmes qui permettent de faire connaître les écarts par rapport aux budgets et aux prévisions à un rythme suffisant pour permettre les réactions appropriées,*
- *rendre compte systématiquement et promptement aux responsables de l'organisation tout nouveau risque ou échec des mesures de maîtrise des risques existantes.*

Les individus devraient :

- *comprendre leur responsabilité pour chaque risque individuel,*
- *comprendre comment ils peuvent contribuer à l'amélioration continue de la gestion des risques,*
- *comprendre que la gestion et la conscience des risques prennent une part déterminante dans la culture de l'organisation,*
- *Rendre compte systématiquement et rapidement aux responsables de l'organisation de tout nouveau risque ou de tout échec des mesures de maîtrise existantes.*

7.2 Compte-Rendu Externe

Une organisation a besoin de rendre compte à ses parties prenantes régulièrement, sur ses politiques de gestion des risques et leur efficacité du point de vue de ses objectifs.

De plus en plus les parties prenantes attendent qu'une organisation fasse la preuve de sa bonne performance non financière dans des domaines tels que les affaires de la société civile, les droits de l'homme, l'emploi, la santé, l'hygiène la sécurité et l'environnement.

Un bon gouvernement d'entreprise exige des organisations une approche méthodique de la gestion des risques qui :

- *protège les intérêts de leurs parties prenantes,*
- *assure que l'instance dirigeante exerce ses fonctions de direction de la stratégie, de création de valeur et de surveillance de la performance de l'organisation,*
- *s'assurer que des dispositifs de maîtrise de la gestion sont en place et fonctionnent correctement.*

Les moyens mis en place pour le compte rendu officiel sur la gestion des risques doivent être clairement exposés et tenues à la disposition des parties prenantes.

Le compte-rendu officiel doit traiter :

- *des méthodes de maîtrise et en particulier de l'attribution des responsabilités pour la gestion du risque*
- *des processus utilisés pour l'identification des risques, et de la manière dont le système de gestion des risques les prend en compte*
- *des principaux systèmes de maîtrise en place pour gérer les risques significatifs*
- *de la surveillance et de l'examen des systèmes en place*

Il convient de rendre compte de toute défaillance significative mises à jour par le système, ou dans le système lui-même, ainsi que des mesures prises pour faire face à ces défaillances.

8. Structure et Administration de la gestion du risque

8.1 Politique de gestion du Risque

La politique de gestion des risques d'une organisation doit présenter son appétence pour le risque et son approche de la gestion des risques. Ce document devrait également définir les responsabilités pour la gestion des risques dans toute l'organisation.

De plus ce texte fera référence à toute exigence légale de compte-rendu, comme par exemple en matière d'hygiène et de sécurité.
Le processus de gestion des risques s'accompagne d'un ensemble intégré d'outils et de techniques valables aux différents stades des activités de l'organisation.

Pour fonctionner efficacement, le processus de gestion des risques exige :

- *l'engagement du directeur général et des directeurs exécutifs de l'organisation,*
- *l'attribution des responsabilités au sein de l'organisation,*
- *l'attribution de ressources appropriées pour la formation et le développement d'une sensibilité renforcée aux risques chez toutes les parties prenantes.*

8.2 Rôle de l'Instance Dirigeante

L'instance dirigeante (par exemple le Conseil d'Administration) porte la responsabilité de déterminer l'orientation stratégique de l'organisation et de créer l'environnement et les structures pour que la gestion des risques s'effectue efficacement.
Il peut s'agir d'un comité exécutif, un comité non-exécutif, un comité d'audit ou toute autre structure adaptée au mode de fonctionnement de l'organisation et capable d'agir en «sponsor» de la gestion des risques.

L'instance dirigeante doit appréhender, au minimum, en évaluant son système de contrôle interne :

- *la nature et l'ampleur des menaces que l'on peut laisser l'organisation supporter dans le cadre de son activité propre,*
- *la probabilité que de tels risques se réalisent,*
- *comment les risques inacceptables doivent être maîtrisés,*
- *la capacité de l'organisation à réduire au minimum la probabilité du risque et son impact sur les affaires,*
- *les coûts et les avantages des activités de maîtrise des risques,*
- *l'efficacité du processus de gestion des risques,*
- *les implications des décisions de l'Instance Dirigeante en terme de risques.*

8.3 Rôle des Unités Opérationnelles

Les responsabilités des Unités Opérationnelles comprennent :

- *la responsabilité principale de la maîtrise du risque au quotidien,*
- *la responsabilité pour leurs directions de promouvoir la sensibilité aux risques dans les unités et d'y faire connaître les objectifs de gestion des risques,*
- *l'obligation de faire un point régulier sur la gestion des risques lors des réunions de direction de manière à examiner les expositions aux risques et à redéfinir les priorités à la lumière de l'analyse des risques,*
- *la responsabilité pour leurs directions de s'assurer que la gestion des risques est intégrée dès la conception des projets et ainsi que pendant tout leur déroulement.*

8.4 Rôle des personnes responsables de la gestion du risque

Selon de la taille de l'organisation la fonction de gestion des risques peut s'étendre d'un simple «promoteur» des risques, à un gestionnaire des risques à temps partiel, voire à un département complet de gestion des risques.

Le rôle de la fonction de gestion des risques doit comprendre les tâches suivantes :

- *définir la politique et la stratégie pour la gestion des risques,*
- *être «promoteur» principal de la gestion des risques au niveau stratégique et opérationnel,*
- *créer une culture de risque au sein de l'organisation, avec les actions de formation appropriée,*
- *établir et la politique de risque internes et les structures [correspondantes] pour les unités opérationnelles,*
- *concevoir et passer en revue les processus de gestion des risques,*
- *coordonner les diverses unités fonctionnelles qui sont amenées à donner un avis sur la gestion des risques au sein de l'organisation,*
- *développer des processus de réponse au risque, y compris des plans d'urgence et de continuité des activités,*
- *préparer les rapports sur les risques pour l'instance dirigeante et les parties prenantes.*

8.5 Rôle de l'Audit Interne

Le rôle de l'Audit Interne est susceptible de différer d'une organisation à l'autre.

Dans la pratique, le rôle de l'Audit Interne peut inclure tout ou partie des points suivants:

- *centrer le travail de l'audit interne sur les risques significatifs, tels qu'identifiés par les responsables de l'organisation ; auditer les processus de gestion du risque dans l'ensemble de l'organisation,*
- *fournir des assurances sur la qualité de la gestion du risque,*
- *soutenir et prendre une part active dans le processus de gestion des risques,*
- *faciliter l'identification /l'évaluation des risques et former le personnel à la gestion des risques et aux dispositifs internes de maîtrise,*
- *coordonner le compte-rendu des risques à l'instance dirigeante et au comité d'audit entre autres.*

En déterminant le rôle le plus approprié, pour une organisation particulière, l'Audit Interne doit s'assurer que les exigences professionnelles d'indépendance et d'objectivité sont respectées.

8.6 Ressources et Mise en Oeuvre

Les ressources nécessaires pour mettre en oeuvre la politique de gestion des risques de l'organisation doivent être clairement établies à chaque niveau de gestion et dans chaque unité opérationnelle.
En plus des autres fonctions opérationnelles qu'ils peuvent avoir, les personnes impliquées dans la gestion des risques doivent avoir des rôles clairement définis dans la coordination de la politique et la stratégie de la gestion des risques. Une définition tout aussi précise est également nécessaire pour les personnes impliquées d'une part dans l'audit et l'examen des dispositifs internes de maîtrise et d'autre part dans la facilitation du processus de gestion des risques.
La gestion des risques doit faire partie intégrante de l'organisation par le biais des processus stratégiques et budgétaires. Son rôle doit être souligné lors de l'intégration des nouveaux employés, lors de toute autre action de formation, tout comme dans le cadre de chaque projet opérationnel comme les développements de produits et de services.

9. Surveillance et Revue du processus de gestion du risque

Une gestion des risques efficace requiert une structure de compte-rendu et de revue pour assurer que les risques sont efficacement identifiés et évalués et que les dispositifs de maîtrise et les réponses appropriées sont en place. Il convient d'auditer régulièrement la conformité à la politique et aux normes, et de passer régulièrement les performances en revue pour identifier les opportunités d'amélioration. Il faut garder à l'esprit que les organisations sont dynamiques et opèrent dans des environnements dynamiques. Les changements dans l'organisation et dans l'environnement dans lequel elle opère doivent être identifiés et les systèmes modifiés en conséquence.
Le processus de surveillance doit fournir l'assurance que les dispositifs de maîtrise appropriés sont en place pour les activités de l'organisation et que les procédures sont comprises et suivies.
Les changements dans l'organisation et l'environnement dans lequel elle opère doivent être identifiés et les systèmes modifiés en conséquence.

Tout procédé de surveillance et de revue doit également déterminer si:

- *les mesures adoptées ont produit les résultats escomptés,*
- *les procédures adoptées et les informations recueillies pour entreprendre l'évaluation étaient appropriées,*
- *Une meilleure connaissance aurait aidé à prendre de meilleures décisions et identifier quelles leçons pourraient être retenues pour l'évaluation et la gestion des risques dans le futur.*

10. Appendice

Techniques d'identification de risque - exemples

- *Brainstorming,*
- *Questionnaires,*
- *[Etudes économiques] qui observent chaque processus et décrivent les processus internes et les facteurs externes qui peuvent influencer ces processus,*
- *Comparaisons sectorielles; (benchmarking),*
- *Analyse de scénario,*
- *Ateliers d'appréciation des risques,*
- *Enquêtes sur les accidents,*
- *Audit et inspection,*
- *HAZOP (Études de Risque et d'Opérabilite)*

Méthodes et techniques d'analyse des risques - exemples

Aléa positif

- *étude de marché,*
- *prospection,*
- *test marketing,*
- *recherche et développement,*
- *analyse d'impact sur l'activité.*

Aléa positif et négatif

- *modèle d'[inter]dépendance,*
- *analyse SWOT forces, faiblesses, opportunités, menaces,*
- *analyse d'arbre d'événement,*
- *planification de continuité de l'activité,*
- *analyse BPEST (affaires, politique, économique, social, technologique),*
- *modélisation des options réelles,*
- *prise de décision dans des conditions de risque et d'incertitude,*
- *inférence statistique,*
- *mesures de moyenne et de variance,*
- *PESTLE (Ambiant Légal Technique Social Économique Politique).*

Aléa négatif

- *analyse des menaces,*
- *analyse de l'arbre des défaillances,*
- *FMEA (analyse des modes et effets des défaillances).*

Notes du traducteur

La traduction s'appuie autant que possible sur le "Guide 73 Iso/Iec, Risk management-vocabulary - guidelines for use in standards".

Le tableau ci-dessous commente par ailleurs certains choix de traduction:

Terme de la version anglaise	Terme français	Commentaire
internal control	système de contrôle interne	
entreprise	organisation	le texte s'applique à toutes les organisations sans perte de sens
the board	l'instance dirigeante	même remarque
stakeholders	parties prenantes	
management	Gestion	
standard	cadre de référence	plus proche de l'intention que "norme" ou "standard"
risk avoidance	évitement du risque	
to control	maîtriser	
knowledge base	capital de connaissance	
downside	aléa négatif	
upside	aléa positif	
reporting	compte-rendu	
formal	officiel	

FOR LOCAL INFORMATION, PLEASE CONTACT THE OFFICE OF THE NATIONAL ASSOCIATION

AGERS - Asociacion Española de Gerencia de Riesgos y Seguros
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.– 28006 Madrid - SPAIN
Tel: + 34-91-562.84.25– Fax: + 34-91-561.54.05– Email: gerencia@agers.es

AIRMIC - The association of Insurance and Risk Managers
Lloyd's Avenue, 6 – London EC3N3AX - UK
Tel: + 44-207-480.76.10 – Fax: + 44-207-702.37.52 – Email: enquiries@airmic.co.uk
Web: www.airmic.com

AMRAE - Association pour le Management des Risques et des Assurances de l'Entreprise
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE
Tel: + 33-1-42.89.33.16 – Fax: + 33-1-42.89.33.14 – Email: amrae@amrae.asso.fr
Web: www.amrae.asso.fr

ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
Viale Coni Zugna, 53 – 20144 Milano - ITALY
Tel: + 39-02-58.10.33.00 – Fax: + 39-02-58.10.32.33 – Email: anra@betam.it
Web: www.anra.it

BELRIM - Belgian Risk Management Association
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM
Tel: + 32-2-380.03.94 – Fax: + 32-2-370.34.93 – Email: info@belrim.com
Web: www.belrim.com

BfV - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften E. V.
Hattenbergstrasse 10, 55122 Mainz - D
Tel. + 49 - 6131 – 662226 - Fax. + 49 - 6131 – 662059 - Email. johannes.fischer@schott.com
Web: www.bfv-fvv.de

DARIM - Dansk Industris Risk Management Forening
DK-1787 Copenhagen – DENMARK
Tel: + 45-33-77.33.77 – Fax: + 45-33-77.33.00 – Email: bg@di.dk

DVS - Deutscher Versicherungs-Schutzverband e.V.
Breite Strasse 98 - D 53111 Bonn - Germany
Tel: + 49-228-98.22.30 - Fax: + 49-228-63.16.51- Email: info@dvs-schutzverband.de
Web: www.dvs-schutzverband.de

NARIM - Nederlandse Associatie van Risk en Insurance Managers
Postbus 65707 – 2506 EA Den Haag – THE NETHERLANDS
Tel: + 31-70-345.74.26 – Fax: + 31-70-427.32.63 – Email: info@narim.com
Web: www.narim.com

SIRM - Swiss Association of Insurance and Risk Managers
Route du Jura, 37- Case Postale, 74 – 1706 Fribourg - SWITZERLAND
Tel: + 41-26-347.12.20 – Fax: + 41-26-347.12.39 – Email: sirm@cfcis.ch
Web: www.sirm.ch

ALARM - The National Forum for Risk Management in the Public Sector
Queens Drive, Exmouth - Devon, EX8 2AY
Tel: 01395 223399 - Fax: 01395 223304 - Email admin@alarm.uk.com - www.alarm-uk.com

IRM - The Institute of Risk Management
6 Lloyd's Avenue - London EC3N 3AX
Tel: 020 7709 9808 - Facsimile 020 7709 0716 - Email enquiries@theIRM.org - www.theirm.org

FOR MORE INFORMATION ABOUT FERMA

FERMA - RUE DE LA PRESSE 4
1000 BRUSSELS - BELGIUM

PHONE: + 32 2 227.11.44
FAX: + 32 2 227.11.48

EMAIL: info@ferma-asso.org
WEB: www.ferma-asso.org